



DEPARTMENT OF THE AIR FORCE  
AIR FORCE OFFICE OF SPECIAL INVESTIGATIONS

HQ AFOSI/XILI  
Attn: FOIA Section  
27130 Telegraph Rd  
Quantico VA 22134

Karl Grindal  
4601 N Fairfax Dr Ste 1200  
Arlington VA 22203

AUG 12 2014

Dear Mr. Grindal

This is in response to your Freedom of Information Act (FOIA) request, dated 11 January 2012, that was originally submitted to the Federal Bureau of Investigations (FBI). During the processing of your request, AFOSI documents were identified and forwarded to our office for processing and direct response to you. We received your request on 28 June 2013 and assigned tracking number 2014-00408-F.

Information from AFOSI criminal investigative records are exempt from release under the Privacy Act, Title 5 United States Code (USC) Section 552(a)(J)(2). In order to provide you the maximum amount of releasable information, we are processing your request under the FOIA. Since portions of the information requested are also exempt from disclosure under the FOIA, we have inserted the exemptions below in the attached document(s).

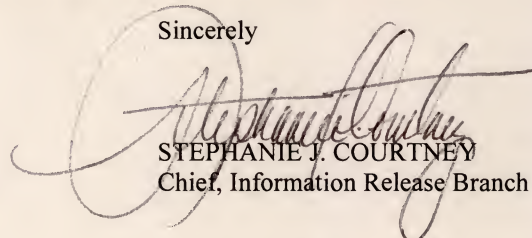
a. Exemption b6 permits the withholding of all information about individuals in "personnel and medical files and similar files" when the disclosure of such information "would constitute a clearly unwarranted invasion of personal privacy."

b. Exemption b7c provides protection for personal information in law enforcement records the disclosure of which "could reasonably be expected to constitute an unwarranted invasion of personal privacy."

The authority for the exemptions used can be found in 5 USC § 552 and in Air Force Manual 33-302, which can be accessed via the Air Force FOIA page at <http://www.foia.af.mil/>.

If you interpret my response as not fully complying with your request, you may appeal this decision with the Secretary of the Air Force by email to [afosi\\_hq\\_foia\\_request@us.af.mil](mailto:afosi_hq_foia_request@us.af.mil), by mail to AFOSI/XILI, ATTN: FOIA Office, 27130 Telegraph Rd, Quantico, VA 22134, or by fax to (571) 305-8229 no later than 60 calendar days from the date of this letter. Include your reason(s) for reconsideration and attach a copy of this letter.

Sincerely



STEPHANIE J. COURTNEY  
Chief, Information Release Branch

Attachment:  
Cy of Referred Documents



# AFOSI ITEM

**DATE:** 8 December 1997**TITLE:** UNAUTHORIZED ACCESS OF MULTIPLE USAF, ARMY, AND NAVY COMPUTER SYSTEMS THROUGH STANFORD UNIVERSITY**AFOSI FILE NUMBER:** 97101D96-S812937**SUBJECT:** (b)(6),(b)(7)(C) Civilian**MALE BORN:** (b)(6),(b)(7)(C) **UNKNOWN**

(b)(6),(b)(7)(C)

**PREVIOUS INFORMATION:** 23 Oct 97

- Scott AFB IL, 3, 4, & 21 May 97: Unauthorized access of USTRANSCOM computer system at Scott AFB (SAFB) by unknown individual(s). Air Force Computer Emergency Response Team (AFCERT) traced the intrusions back to Peoples Republic of China (PRC).
- Compromised system consisted of two computers. Information extracted from computers was: Host File, file containing user IDs (but no passwords), and the message of the day.
- On 26 May 97, another computer system on SAFB belonging to HQ AMC/SCMVF (Forms Management Office) was accessed by an unauthorized user. AFCERT traced the intrusion back to Stanford University (SU).
- The function of the computer was as a File Transfer Protocol (FTP) server, so Air Force customers could download AF forms and publications from bases worldwide.
- On 30 May 97 computer systems at both Andersen AFB and Minot AFB were compromised by an unknown individual(s) through the SU system.
- Access at Minot AFB was gained using a Gunter AFB (GAFB) maintenance account. Account is used to access approximately 280 computers in the AF (primarily medical systems, i.e., Expense Assignment System [EAS] system). Passwords/logins are the same on all systems.

DISSEMINATION OF THE INFORMATION IN THIS ITEM SHOULD BE LIMITED IN ORDER TO PROTECT THE IDENTITIES AND PRESERVE THE RIGHTS OF THE INDIVIDUAL(S) UNDER INVESTIGATION.

~~SPECIAL HANDLING REQUIRED~~  
(AFOSII 71-101). REPRODUCTION IS NOT AUTHORIZED.

~~FOR OFFICIAL USE ONLY~~

**DISTRIBUTION:**



**(Continuation Sheet)**

- Access at Anderson AFB was gained into the Fuels Automated Management System (FAMS) by using a valid account and password. This system pulls fuel transaction data from the Automated Fuels Service Station.
- Investigation disclosed:
  - Computer logs provided by SU linked the 21 May 97 TRANSCOM computer intrusion at SAFB to the other computer intrusions.
  - From 21 May 97 through 13 Jun 97, perpetrator(s) utilized the computer at SU to launch attempts to gain unauthorized access into numerous USAF, US Navy, and US Army computer systems.
  - All the affected systems were unclassified. When attacks were successful, Subject(s) used valid passwords and accounts; however, they were not authorized to use these accounts. It is unknown how Subject(s) attained these valid accounts.
  - Analysis of Subject(s) computer targets demonstrated no pattern.
  - The computer logs from SU indicated the attacks launched from SU during all of the computer intrusion activity is traced one leg back to China. This does not necessarily mean the Subject(s) started their attacks from within the PRC.
- Specialized investigative techniques identified Subject.

**UPDATED INFORMATION:**

- Subject's supervisor, USMC active duty LTC, was interviewed and related:
  - He had observed Subject accessing SU computer system from the US Government computer terminal on Camp Courtney, Japan. He provided a user name he believed Subject had used to access SU computers.
  - He provided names of 3 other Science Applications International Corporation (SAIC) employees he believed were involved in hacker activity.
  - Subject had access to USMC, USN classified information.
- Subject has been interviewed on several occasions, beginning on 22 Oct 97:
  - Naval Criminal Investigative Service present at all interviews.
  - Subject stated he had not passed classified information to anyone and had not transferred classified information to a unclassified system.
  - Subject stated he was given the passwords and user names of the accounts he hacked (USAF/USN/USA), but would not identify the source.



**(Continuation Sheet)**

- Subject was given a criminal polygraph on 29 Oct 97. Results were deception indicated in regards to questions pertaining to computer intrusions at SAFB and into one Navy site in San Diego CA.
- Subject was given a Counterintelligence Scope Polygraph on 30 Oct 97. Results were no deception indicated to questions pertaining to relevant counterintelligence issues.
- Additional interviews and extensive computer media analysis is ongoing. Analysis of systems includes looking for indications of trojan horses and other malicious code that could have been introduced onto the affected systems.
- Subject terminated his employment with SAIC.
- Investigation continues.
- 375 AW/CC, USTRANSCOM/CC/SSO and AMC/CC/CV have been briefed.
- FBI, San Francisco International Computer Crime Squad, SU Police Dept , and U.S. Attorney have been briefed and are providing assistance.
- This item was provided to AMC/CC/CV/SC and USTRANSCOM/CC/CISO-J2/J6.
- POC at Region 3 is SA (b)(6),(b)(7)(C), DSN: (b)(6),(b)(7)(C)